FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

January 23, 2014

Mr. Gregg Steinhafel
Chairman, President, and Chief Executive Officer
Target Corporation
1000 Nicollet Mall
Minneapolis, MN 55403

Dear Mr. Steinhafel:

On December 19, 2013, Target announced that credit card and debit card information for approximately 40 million customers had been compromised in a massive cybersecurity breach. According to Target, criminals "forced their way" into network systems, gaining access to sensitive payment card data including card numbers and encrypted pin numbers.[1] On January 10, Target acknowledged that another trove of data – names, addresses, email addresses, and phone numbers – affecting as many as 70 million customers had also been compromised.

The Committee will be holding a hearing on this breach and the overall impact of data breaches on consumers during the first week of February. We are writing to seek information needed by the Committee prior to the hearing in order to improve our understanding of the causes and impacts of the December data breach affecting Target consumers.

This breach is particularly significant because of its unprecedented scope and scale. More than one-fifth of Americans may be affected by the Target breach. It has been estimated that the costs to banks and retailers could exceed $18 billion and that "consumers could be liable for more than $4 billion in uncovered losses and other costs."[2] While the immediate concerns relate to securing customer information and preventing fraudulent charges, there are many unanswered questions about this cyberattack and its implications for consumer privacy and data security.

---

[1] *Data Breach FAQ*, Target (accessed Jan. 20, 2014) (online at corporate.target.com/about/shopping-experience/payment-card-issue-FAQ#q5888).

[2] *A Sneaky Path Into Target Customers' Wallets*, New York Times (Jan. 17, 2014) (online at www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html).

Questions remain about how exactly this attack was carried out, who was responsible, whether it could have been prevented, how Target responded, and how retailers and customers can protect themselves going forward. Reuters has reported that "Visa Inc issued two alerts [in April and August] last year about a surge in cyber attacks on retailers that specifically warned about the threat from memory parsing malware."[3] Despite these warnings, the *New York Times* reported that the criminals responsible "discovered that Target's systems were astonishingly open – lacking the virtual walls and motion detectors found in secure networks like many banks'."[4] And security experts have found that the hackers may have been able to break into systems at Target and other stores as a result of weak passwords on point-of-sale systems.[5]

Other reports have also raised questions about the timing and adequacy of disclosure of the breach.[6] Information that Target has provided to the Committee raises additional questions about the timing of the breach and subsequent public disclosure. For example, in a January 17, 2014, briefing with Democratic staff, Target officials informed staff that the company discovered and disabled malware responsible for the breach on December 15, 2013. But the *New York Times* reported that Target officials were informed of the breach two days earlier, on December 13, 2013.[7]

In order that we may fully understand prior to our Committee hearing how this theft of confidential customer information occurred, we ask that you please provide the following information and documents no later than January 31, 2014:

---

[3] *Exclusive: More well-known U.S. retailers victims of cyber attacks – sources*, Reuters (Jan. 12, 2014) (online at www.reuters.com/article/2014/01/12/us-target-databreach-retailers-idUSBREA0B01720140112).

[4] *A Sneaky Path Into Target Customers' Wallets*, New York Times (Jan. 17, 2014) (online at www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html).

[5] *The teenager is the author of BlackPOS/Kaptoxa malware (Target), several other breaches may be revealed soon*, IntelCrawler (Jan. 17, 2014) (online at intelcrawler.com/about/press08).

[6] *U.S. companies allowed to delay disclosure of data breaches*, Reuters (Jan. 16, 2014) (online at www.reuters.com/article/2014/01/16/us-target-data-notification-idUSBREA0F1LO20140116).

[7] *A Sneaky Path Into Target Customers' Wallets*, New York Times (Jan. 17, 2014) (online at www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html); Briefing by Scott Kennedy, President, Financial and Retail Services, Target, to House Energy & Commerce Minority Staff (Jan. 17, 2014).

1. All written policies or guidelines relating to threat monitoring, network security, or point-of-sale system protection, including any strategies to protect against threats posed by memory-parsing malware, from January 1, 2012, to the present.

2. All documentation, pertaining to fiscal year 2013 and dated prior to November 27, 2013, detailing the funds spent and persons employed on the network security of systems serving Target stores. Please indicate whether or not additional funds were spent or additional network security personnel hired to protect the integrity of systems serving Target stores during the holiday season. Please provide comparable documentation for individual fiscal year data for fiscal years 2007-2012.

3. All email correspondence, analyses, reports, or any other communications relating to the Kaptoxa malware, or to point-of-sale system security or any other information security systems implicated in this breach for Target officials from January 1, 2012, to the present. Please detail whether Target was previously aware of any potential vulnerabilities to its point-of-sale systems or any other systems implicated in this breach. Please include all documents, including email correspondence for Target officials from January 1, 2013, to the present, relating to Visa's April and August 2013 alerts regarding memory-parsing malware.

4. All documents relating to Target's response and public notification activities relating to the breach. Please provide a detailed written timeline of when Target was notified of the attacks and of Target's response and public notification activities from December 1, 2013, to the present. Please detail when, how, and by whom Target was first made aware of a potential security breach.

We understand that much of this information is sensitive in nature, and that Target and law enforcement officials are conducting ongoing investigations of the breach. The Committee has a long history of working with confidential and classified material in a sensitive manner, and we are happy to work with you and your staff to ensure that this is the case in this investigation.

Sincerely,

Henry A. Waxman
Ranking Member

Diana DeGette
Ranking Member
Subcommittee on Oversight and Investigations

Jan Schakowsky
Ranking Member
Subcommittee on Commerce, Manufacturing, and Trade